Test 1, take-home
due on Tuesday, April 1

Problem 1. Find the minimal polynomial of $\sqrt[3]{2}+\sqrt[3]{4}$ over $\mathbb{Q}$. What are the other roots of this polynomial?

Solution: Let $a=\sqrt[3]{2}+\sqrt[3]{4}$. Let f be the minimal polynomial of a over $\mathbb{Q}$ and let K be a splitting field of x^3-2 over $\mathbb{Q}$. Clearly $a\in K$. Let u be the primitive 3-rd root of 1, so $\sqrt[3]{2}$, $u\sqrt[3]{2}$, and $u^2\sqrt[3]{2}$ are the roots of x^3-2 in K. It follows that $u\in K$. From Galois theory, there are authomorphisms σ, τ of $K/\mathbb{Q}$ such that $\sigma(\sqrt[3]{2})=u\sqrt[3]{2}$ and $\sigma(\sqrt[3]{2})=u^2\sqrt[3]{2}$ (since x^3-2 is irreducible over $\mathbb{Q}$). Note that $\sqrt[3]{4}=\sqrt[3]{2}^2$. It follows that $\sigma(a)=u\sqrt[3]{2}+u^2\sqrt[3]{4}$ and $\tau(a)=u^2\sqrt[3]{2}+u\sqrt[3]{4}$ are roots of f. Note that

$$(x-a)(x-\sigma(a))(x-\tau(a))=x^3-(a+\sigma(a)+\tau(a))x^2+(a\sigma(a)+a\tau(a)+\sigma(a)\tau(a))x-a\sigma(a)\tau(a).$$

Now $a+\sigma(a)+\tau(a)=(1+u+u^2)(a+a^2)=0$, $a\sigma(a)+a\tau(a)+\sigma(a)\tau(a)=-6$, $a\sigma(a)\tau(a)=6$ so

$$(x-a)(x-\sigma(a))(x-\tau(a))=x^3-6x-6$$

. It follows that x^3-6x-6 is the minimal polynomial of a.

Another solution: Clearly $a\in M=\mathbb{Q}(\sqrt[3]{2})$, so the degree of a over $\mathbb{Q}$ is a divisor of $[M:\mathbb{Q}]=3$. Note that 1, $\sqrt[3]{2}$, $\sqrt[3]{2}^2=\sqrt[3]{4}$ is a basis of $M/\mathbb{Q}$. Thus $a=\sqrt[3]{2}+\sqrt[3]{4}$ is not in $\mathbb{Q}$ and hence it has degree 3 over $\mathbb{Q}$. Note that

$$a^2=(\sqrt[3]{2}+\sqrt[3]{4})^2=4+2\sqrt[3]{2}+\sqrt[3]{4}$$

and

$$a^3=(\sqrt[3]{2}+\sqrt[3]{4})^3=2+6\sqrt[3]{2}+6\sqrt[3]{4}+4=6(1+a).$$

Thus $a^3-6a-6=0$, so $x^3-6x-6$is the minimal polynomial of a over $\mathbb{Q}$.

Problem 2. Let L/K be a finite extension of fields. Suppose that $f\in K[x]$ is irreducible over K and its degree is relatively prime to $[L:K]$. Prove that f is irreducible in $L[x]$.

Solution: Let F be a field extension of L in which f has a root a. Since f is irreducible in $K[x]$, we have $[K(a):K]=d$, where d is the degree of f. Let

$m = [L(a) : L]$, so clearly $m \leq d$. Then $[L(a) : K] = m[L : K]$. On the other hand, $[L(a) : K] = [L(a) : K(a)][K(a) : K] = d[L(a) : K(a)]$. Thus $d|m[L : K]$, and since d and $[L : K]$ are relatively prime, we have $d|m$. But $m \leq d$, so we must have $m = d$. This means that the minimal polynomial of a over L has degree d and therefore f is the minimal polynomial of a over L. In particuler, f is irreducible over L.

Problem 3. Let $\Phi_n(x)$ be the $n-$th cyclotomic polynomial and let p be a prime number.

a) Prove that if $p|n$ then $\Phi_{pn}(x) = \Phi_n(x^p)$.

b) Prove that if $p \nmid n$ then $\Phi_n(x^p) = \Phi_n(x)\Phi_{np}(x)$.

Solution: Let u be a primitive np-th root of 1. Then u^p is a primitive n-th root of 1 so $\Phi_n(u^p) = 0$. It follows that every root of Φ_{np} is a root of $\Phi_n(x^p)$, so $\Phi_{np}|\Phi_n(x^p)$. If $p|n$, then $\phi(np) = p\phi(n)$, so Φ_{np} and $\Phi_n(x^p)$ have the same degree and are both monic. It follows that $\Phi_{pn}(x) = \Phi_n(x^p)$ which proves a).

Suppose now that $p \nmid n$. If w is a primitive n-th root of 1, then w^p is also a primitive n-th root of 1. Thus $\Phi_n(w^p) = 0$. We see that every root of Φ_n is also a root of $\Phi_n(x^p)$. Thus $\Phi_n|\Phi_n(x^p)$. Since Φ_n and Φ_{np} are relatively prime, we see that $\Phi_n(x)\Phi_{np}(x)|\Phi_n(x^p)$. But both $\Phi_n(x)\Phi_{np}(x)$ and $\Phi_n(x^p)$ are monic and have degree $\phi(np) = \phi(n)\phi(p)$, so we must have $\Phi_n(x^p) = \Phi_n(x)\Phi_{np}(x)$. This proves b).

Problem 4. Let L be a field and let p be a prime number. Suppose that F_1, F_2, K are subfields of L such that F_1/K and F_2/K are Galois and both $Gal(F_1/K)$ and $Gal(F_2/K)$ are p-groups. Prove that the Galois groups of F_1F_2/K and $F_1 \cap F_2/K$ are also p-groups.

Solution: Let $L = F_1F_2$. Since both F_1/K and F_2/K are Galois, so is L/K. Let $G = Gal(L/K)$ and let H_1, H_2 be the subgroups corresponding to F_1, F_2 respectively (so $H_i = Gal(L/F_i)$, $i = 1, 2$). Thus $H_i \lhd G$ and G/H_i is isomorphic to $Gal(F_i/K)$, $i = 1, 2$. Thus G/H_1 and G/H_2 are p-groups. Rcall that $Gal(F_1F_2/K)$ is isomorphic to $G/H_1 \cap H_2$ and $Gal(F_1 \cap F_2/K)$ is isomorphic to G/H_1H_2.

Thus we reduced the problem to a problem about groups: if H_1, H_2 are normal subgroups of a group G such that G/H_1 and G/H_2 are p-groups then $G/H_1 \cap H_2$ and G/H_1H_2 are also p-groups.

Note that there is a surjective homomorphism $G/H_i \longrightarrow G/H_1H_2$ which sends a coset gH_i to the coset $g(H_1H_2)$ (i=1,2). Since an image of a p-group under a homomorphism is also a p-group (why?), we see that G/H_1H_2 is a p-group.

To see that $G/H_1 \cap H_2$ is a p-group recall the following very useful observation: the group $G/H_1 \cap H_2$ is isomorphic to a subgroup of $G/H_1 \times G/H_2$. In fact, it is easy to check that the map which sends a coset $g(H_1 \cap H_2)$ to the pair (gH_1, gH_2) is an injective homomorphism $G/H_1 \cap H_2 \longrightarrow G/H_1 \times G/H_2$ (see Problem 2d) from Homework 37 of Math 401 for more details). Since a product of two p groups is a p-group and a subgroup of a p-group is also a p-group, we see that $G/H_1 \cap H_2$ is a p-group.

Problem 5. a) Prove that the Galois group of the splitting field of $x^3 - 3$ over $\mathbb{Q}$ is isomorphic to the symmetric group S_3 hence is nonabelian.

b) Prove that $\mathbb{Q}(\sqrt[3]{3})$ is not a subfield of any cyclotomic field $\mathbb{Q}(\zeta_n)$.

Solution: a) Let L be a splitting field of $x^3 - 3$ over $\mathbb{Q}$. Let $a = \sqrt[3]{3}$ and let u be a primitive 3-rd root of 1. Then a, ua, u^2a are the roots of $x^3 - 3$ so $L = \mathbb{Q}(a, u)$. Note that $[\mathbb{Q}(a) : \mathbb{Q}] = 3$, since $x^3 - 3$ is irreducible over $\mathbb{Q}$. Since $\mathbb{Q}(a)$ consists ot real numbers and u is not real, we have $u \notin \mathbb{Q}(a)$. Since u is of degree 2 over $\mathbb{Q}$, we must have $[\mathbb{Q}(a, u) : \mathbb{Q}(a)] = 2$ and $[\mathbb{Q}(a, u) : \mathbb{Q}] = 6$. Thus the Galois group G of $L/\mathbb{Q}$ has order 6. Note that G permutes the roots of $x^3 - 2$ so it can be identified with a subgroup S_3. But both G and S_3 have order 6, so G is isomorphoic to S_3. In particular, G is not abelian.

b) Suppose that $\mathbb{Q}(\sqrt[3]{3})$ is a subfield of some cyclotomic field $\mathbb{Q}(\zeta_n)$. Recall that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois. Thus $x^3 - 2$ must have all its roots in $\mathbb{Q}(\zeta_n)$, so $L \subseteq \mathbb{Q}(\zeta_n)$. Let A be the Galois group $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and let B be the subgroup corresponding to L (so $B = Gal(\mathbb{Q}(\zeta_n)/L)$). Since $L/(\mathbb{Q}$ is Galois, we have $B \lhd A$ and G is isomorphic to A/B. Recall that A is abelian, which implies that A/B is abelian. Thus G is abelian, which contradicts a). Our assumption that $\mathbb{Q}(\sqrt[3]{3})$ is a subfield of some cyclotomic field $\mathbb{Q}(\zeta_n)$ is then false.